CLAIMS

What is claimed is:

1.   A method of securely allocating mobile devices to at least one user, comprising the steps of:

storing a plurality of mobile devices in an inoperative state under the control of a host computer;

accepting as an input an identification code; and

the host computer selectively placing a mobile device among the plurality of mobile devices in an operative state based on the identification code.

2.   The method of claim 1, further comprising the steps of:

storing the plurality of mobile devices in a secure area; and

granting a user access to the secure area based on the identification code.

3.   The method of claim 2, wherein the step of storing the plurality of mobile devices in a secure area includes storing the plurality of mobile devices in a secure enclosure.

4.   The method of claim 2, wherein the step of storing the plurality of mobile devices in a secure area includes storing the plurality of devices in a secure room.

5.   The method of claim 2, wherein the step of granting access to the secure area based on the identification code includes identification codes selected from the group consisting of numeric codes, alpha-numeric codes, voiceprints, fingerprints and iris patterns.

6.   The method of claim 1, further comprising the step of:

selecting a mobile device from the plurality of mobile devices that will be placed in an operative state based on a preselected criteria.

7.   The method of claim 6, wherein the step of selecting a mobile device from the plurality of mobile devices that will be placed in an operative state based on a preselected criteria includes criteria selected from the group

consisting of prior history of use, position within an organization, current battery charge level, available software on the device, and user preference.

8. The method of claim 1, further comprising the step of:
configuring the operational mobile device to be operational for a first interval, where upon expiration of the first interval the mobile device becomes inoperational.

9. The method of claim 8, further comprising the step of:
configuring the operational mobile device to retain data within a memory area for a second interval, where upon expiration of the second interval all data within the memory area is purged.

10. The method of claim 9, further comprising the step of:
returning the mobile device to the secure area prior to the expiration of the second interval, thereby preventing the data stored in the memory area from being purged.

11. The method of claim 1, further comprising the step of:
configuring the operational mobile device to retain data within a memory area for a first interval, where upon expiration of the first interval all data within the memory area is purged.

12. The method of claim 1, further comprising the step of:
monitoring when a new mobile device operating software is available; and upgrading each mobile device with the new operating software.

13. The method of claim 1, further comprising the step of:
customizing a selected mobile device's operations based on the particular user.

14. The method of claim 1, further comprising the step of:
displaying an advertisement on the selected mobile device based on a previous history of the particular user.

15. The method of claim 1, further comprising the step of:

emitting an alarm when the user selects a mobile device that is in the inoperative state.

16. The method of claim 15, wherein the step of emitting an alarm includes emitting an audible alarm.

17. The method of claim 15, wherein the step of emitting an alarm includes emitting a visual alarm.

18. The method of claim 1, further comprising the step of:
establishing a communicans link between a first selected mobile device and a second selected mobile device, wherein messages are exchanged between the users of each mobile device.

19. The method of claim 18, wherein the step of establishing a communication link includes communicating directly from the first mobile device to the second mobile device.

20. The method of claim 18, wherein the step of establishing a communication link includes communicating indirectly from the first mobile device to the second mobile device.

21. The method of claim 20, wherein the step of communicating indirectly includes communicating from the first mobile device to the host computer to the second mobile device.

22. The method of claim 1, further comprising the step of:
tracking the location of the selected mobile device as the selected mobile device moves between a plurality of cells.

23. The method of claim 22, wherein the step of tracking the location of the selected mobile device includes storing the selected mobile device location in a memory.

24. The method of claim 1, further comprising the step of:
instructing the selected mobile device to emit an alert signal to assist in locating the mobile device.

25.   A method of securely allocating mobile devices to at least one user, comprising the steps of:

storing a plurality of mobile devices in a secure area, access to the secure area being under the control of a host computer;

accepting as an input an identification code; and

the host computer granting the user access to the secure area based on the identification code.

26.   The method of claim 25, wherein the step of storing the plurality of mobile devices in a secure area includes storing the plurality of mobile devices in a secure enclosure.

27.   The method of claim 25, wherein the step of storing the plurality of mobile devices in a secure area includes storing the plurality of mobile devices in a secure room.

28.   The method of claim 25, wherein the step of the host computer granting access to the secure area based on an identification code includes identification codes selected from the group consisting of numeric codes, alpha-numeric codes, voiceprints, fingerprints and iris patterns.

29.   A mobile device allocation system for securely allocating mobile devices to a plurality of users, comprising:

at least one system backbone;

at least one host computer coupled to the system backbone; and

a plurality of mobile terminals operatively configured to communicate to the host computer through the system backbone,

wherein the plurality of mobile devices are stored in an inoperative state, and the at least one host computer and a selected mobile device are operatively configured to place the selected mobile device in an operative state based upon an identification code.

30.   The system of claim 29, further comprising:

at least one secure area, wherein the plurality of mobile devices are stored in the at least one secure area, and the at least one host computer is operatively

configured to grant access to the at least one secure area based on the identification code.

31.   The system of claim 30, wherein the secure area is a secure room.

32.   The system of claim 30, wherein the secure area is a secure enclosure.

33.   The system of claim 30, wherein the identification code is selected from the group consisting of numeric codes, alpha-numeric codes, voiceprints, fingerprints and iris patterns.

34.   The system of claim 30, further comprising:
a plurality of docking stations located in the at least one secure area, wherein each docking station is coupled to the at least one system backbone, and each mobile device is operatively configured to communicate to the host computer through a respective docking station.

35.   The system of claim 34, further comprising:
at least one wireless remote station coupled to the at least one system backbone, wherein each mobile terminal is operatively configured to communicate to the host computer through the wireless remote station when the respective mobile device is not in the docking station.

36.   The system of claim 29, wherein the at least one host computer selects the mobile device to be placed in an operative state based on a preselected criteria.

37.   The system of claim 36, wherein the preselected criteria is selected from the group consisting of prior history of use, position within an organization, current battery charge level, available software on the device, and user preference.

38.   The system of claim 29, wherein the operational mobile device is configured to be operational for a first interval, and upon expiration of the first interval the operational mobile device becomes inoperational.

39.   The system of claim 38, wherein the operational mobile device is configured to retain data within a memory area for a second interval, and upon expiration of the second interval all data within the memory area is purged.

40.   The system of claim 39, wherein the second interval is inhibited if the mobile device is returned to the secure area prior to the expiration of the second interval.

41.   The system of claim 29, wherein the operational mobile device is configured to retain data within a memory area for a second interval, and upon expiration of the second interval all data within the memory area is purged.

42.   The system of claim 29, wherein the host computer monitors when a new mobile device operating software is available, and upon detecting a new operating software, the host computer transmits the operating software to a respective mobile device.

43.   The system of claim 29, wherein the host computer configures the selected mobile device's functionality based on the particular user.

44.   The system of claim 29, wherein the mobile device displays advertisements based on a previous history of the particular user.

45.   The system of claim 29, wherein an alarm is emitted when the user selects an inoperative mobile terminal.

46.   The system of claim 45, wherein the alarm is an audible alarm.

47.   The system of claim 45, wherein the alarm is a visual alarm.

48.   The system of claim 29, further comprising:
a communicans link between a first mobile device and a second mobile device, wherein messages are exchanged over the communications link between the user of the first mobile device and the user of the second mobile device.

49.   The system of claim 48, wherein the communications link is a direct communications link from the first mobile device to the second mobile device.

50.   The system of claim 48, wherein the communications link is an indirect link from the first mobile device to the second mobile device.

51.   The system of claim 50, wherein the indirect communications link includes communicating from the first mobile device to the host computer to the second mobile device.

52.   The system of claim 29, wherein the host computer tracks the location of the mobile device as the mobile device moves between a plurality of cells.

53.   The system of claim 52, wherein the host computer stores the location of the mobile device in a memory.

54.   The system of claim 29, wherein the host computer instructs the mobile device to emit an alert signal to assist in locating the mobile device.

55.   The system of claim 29, further comprising:
a remote communication link, wherein at least one mobile device communicates to the host computer through the remote communication link.

56.   The system of claim 55, wherein the remote communication link is an internet connection.

57.   The system of claim 55, wherein the remote communication link is an intranet connection.

58.   The system of claim 55, wherein the remote communication link is a wireless communication link.

59.   A mobile device allocation system, comprising:
at least one secure area;
at least one system backbone;
at least one host computer coupled to the system backbone; and
a plurality of mobile devices operatively configured to communicate to the host computer through the system backbone,

wherein the plurality of mobile devices are stored in the at least one secure area, and the at least one host computer is operatively configured to grant access to the at least one secure area based on a valid identification code.

60.   The system of claim 59, wherein the secure area is a secure room.

61.   The system of claim 59, wherein the secure area is a secure enclosure.

62.   The system of claim 59, wherein the identification code is selected from the group consisting of numeric codes, alpha-numeric codes, voiceprints, fingerprints and iris patterns.